

>

This page walks you through accessing the Security Command Center **Assets** display to review your organization's Google Cloud resources.

To access the Security Command Center assets display, you must have an Cloud Identity and Access Management (Cloud IAM) role that includes the permissions of the **Security Center Assets Viewer** role.

For more information about Security Command Center Cloud IAM roles, see [Access control](/security-command-center/docs/access-control) (/security-command-center/docs/access-control).

To access the assets display:

1. Go to the **Security Command Center** page in the Cloud Console.

[Go to the Security Command Center](https://console.cloud.google.com/security/command-center/dashboard) (https://console.cloud.google.com/security/command-center/dashboard)

2. Select the organization you want to review.
3. On the Security Command Center dashboard that appears, click the **Assets** tab.

The Security Command Center assets detailed list view is displayed.

The assets display enables you to view assets for the entire organization or you can view assets only within a specific project, asset type, or change type. For a detailed view of attributes, resource properties, and findings on a specific asset, click the asset name under the **resourceProperties.name** column.

Assets are automatically scanned two times each day. You can also start an asset scan manually using the Security Command Center dashboard. The `updateTime` value might vary for results within a given automatic or manual scan. This variance is typically less than 10 minutes.

Asset inventory freshness depends on discovery and indexing of the asset source:

- Freshness is usually <1 minute for pre-existing assets.
- Assets that haven't been discovered and indexed in a daily or manual scan will appear in asset inventory after the asset they're attached to is discovered and indexed.

By default, assets are displayed in the organization and project hierarchy. To view assets associated with a specific resource, under **View by Project**, select the organization or project you want to review.

To view your assets grouped by resource type, under the **Assets** tab, click **Asset type**. Assets are displayed in categories like application, bucket, project, and service. The following asset types are currently supported:

- Resource Manager
 - Organization
 - Folder
 - Project
- App Engine
 - Application
 - Service
 - Version
- Compute Engine
 - Address
 - Autoscaler
 - BackendBucket
 - BackendService
 - BillingAccount
 - Disk
 - Firewalls
 - GlobalAddress

- HealthCheck
- HttpHealthCheck
- HttpsHealthCheck
- Image
- Instance
- InstanceGroup
- InstanceTemplate
- License
- Network
- Route
- SecurityPolicy
- Snapshot
- SslCertificate
- Subnetwork
- TargetHttpProxy
- TargetHttpsProxy
- TargetSslProxy
- TargetTcpProxy
- TargetPool
- TargetVpnGateway
- UrlMap
- VpnTunnel
- Cloud DNS
 - ManagedZone
 - Policy
- Cloud IAM
 - ServiceAccount
- Cloud Spanner

- Database
 - Instance
- Cloud Storage
 - Bucket
- Google Kubernetes Engine
 - Cluster
- Container Registry
 - Image

using VPC Service Controls currently blocks Security Command Center asset discovery inside VPC Service perimeters for the following asset types:

Compute Engine

- Addresses
- Routes
- VPN Tunnels

Cloud Storage Buckets

GKE Clusters

For more information about troubleshooting access issues, see [VPC Service Controls Troubleshooting](#) ([service-controls/docs/troubleshooting](#)). To work around the access to these assets, see [Granting access from the internet to VPC Service Controls](#) ([/vpc-service-controls/docs/use-access-levels](#)).

To view individual resources for a specific asset type, under **View by Asset type**, select the asset type you want to review. All assets in that category are displayed in the middle panel. To view details of a specific asset, click the asset.


To view new and deleted assets, under the **Assets** tab, click **Asset changed**. All assets are displayed, including subgroups for new and deleted assets. You can select a time range for which results are displayed by clicking the drop-down list at the top of the assets list.

Security Command Center displays Cloud IAM policies for assets on the **Assets** tab under the **iamPolicy** column. To view Cloud IAM policy details for a specific asset, click **Show/Hide** next to the asset. Cloud IAM policies are also displayed on the asset details panel when you click the asset name under the **resourceProperties.name** column.

By default, the assets display includes the following columns:

- Asset name: `resourceProperties.name`
- Asset type: `securityCenterProperties.resourceType`
- Asset owner: `securityCenterProperties.resourceOwners`
- Resource name: `name`
- Any marks added to the asset: `securityMarks.marks`


You can hide any column except for `resourceProperties.name`, and you can select more asset detail columns to display:

1. To select the asset columns you want to display, click **Columns**. 
2. In the menu that appears, select the columns you want to display.
3. To hide a column, click the column name to clear it.

To save your column selections, click **Remember Columns**. Your column selections apply to all of the views in the **Assets** tab. When you select columns, the Cloud Console URL updates, so you can share the link for a custom view.

Column selections are preserved the next time you view the dashboard, and if you change organizations. To clear all custom column selections, click **Reset Columns**.

To control the screen space for the Assets display, you can change the following options:

- Hide the Cloud Console **Security** side panel by clicking the left arrow. 
- Resize the asset display columns by dragging the dividing line left or right.
- Hide the **Select an asset** side panel by clicking **Hide Info Panel**.

To change the date and time of the results that the assets display includes, click the date and time drop-down, then select the date and time you want.

To sort the assets display, click the column heading for the value by which you want to sort. Columns are sorted by numeric and then alphabetical order.

This section describes how to run common queries to review your resources using Security Command Center.

You can only select these filters in the Security Command Center dashboard if your organization has the related resource type. If you receive the "Choose one of the suggested keys" error message, your organization might not have that resource type.

1. Go to the Security Command Center **Assets** page in the Cloud Console.

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box:

- a. Type `resourceProperties.ac1:allUsers`, and then press **Enter**.
- b. Click the **Filter by** text box, and then select **OR** on the drop-down list.
- c. Type `resourceProperties.ac1:allAuthenticatedUsers`, and then press **Enter**.

The following filter finds firewall rules with SSH port 22 open from any network.

1. Go to the Security Command Center **Assets** page in the Cloud Console.

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box:

- a. Type `resourceProperties.allowed:22`, and then press **Enter**.
- b. Click the **Filter by** text box, and then select **OR** on the drop-down list.
- c. Type `resourceProperties.sourceRange:0.0.0.0/0`, and then press **Enter**.

1. Go to the Security Command Center **Assets** page in the Cloud Console.

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box, enter `resourceProperties.networkInterface:externalIP`.

1. Go to the Security Command Center **Assets** page in the Cloud Console.

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box, enter `-securityCenterProperties.resourceOwners:@[YOUR_DOMAIN]`.

1. Go to the Security Command Center **Assets** page in the Cloud Console.

[Go to the Assets page](https://console.cloud.google.com/security/assets) (https://console.cloud.google.com/security/assets)

2. In the **Filter by** text box, enter `resourceProperties.disk:licenses`.

3. On the list of displayed resources, click **Column display options**, and then select **resourceProperties.disk**.

- Learn how to [use Security Command Center security marks](/security-command-center/docs/how-to-security-marks) (/security-command-center/docs/how-to-security-marks).
- Learn more [about Security Command Center](/security-command-center/docs/concepts-overview) (/security-command-center/docs/concepts-overview).
- Learn how to [read findings](/security-command-center/docs/how-to-findings) (/security-command-center/docs/how-to-findings).